

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-32372  
(P2002-32372A)

(43) 公開日 平成14年1月31日 (2002.1.31)

(51) Int.Cl. <sup>7</sup>	識別記号	FI	テーマコード <sup>*</sup> (参考)
G 0 6 F 17/30	1 2 0	G 0 6 F 17/30	1 2 0 B 5 B 0 1 7
	1 1 0		1 1 0 F 5 B 0 7 5
	1 7 0		1 7 0 Z 5 B 0 8 2
12/00	5 3 7	12/00	5 3 7 A
12/14	3 1 0	12/14	3 1 0 K
審査請求 有 請求項の数13 OL (全 14 頁)			

(21) 出願番号 特願2000-215453(P2000-215453)

(22) 出願日 平成12年7月17日 (2000.7.17)

(71) 出願人 500248320

株式会社エグゼコミュニケーションズ  
東京都渋谷区桜丘町2-6 フルキャスト  
ビル4階

(72) 発明者 油屋 康

東京都渋谷区桜丘町2-6 フルキャスト  
ビル4階 株式会社エグゼコミュニケーションズ内

(74) 代理人 100099324

弁理士 鈴木 正剛

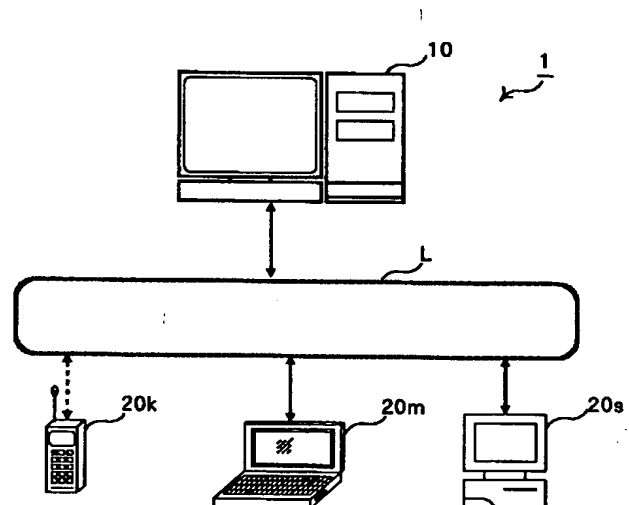
Fターム(参考) 5B017 AA03 BA06 CA16  
5B075 KK43 KK54 KK63 ND20 PQ02  
PQ48 UU08  
5B082 EA11 GA11

(54) 【発明の名称】 個人情報管理方法及びシステム、記録媒体

(57) 【要約】

【課題】 自分の個人情報を他人に安全且つ効率的に伝達することができる個人情報管理システムを提供する。

【解決手段】 操作端末20を用いて不特定の者がアクセス可能なインターネットLに個人情報管理システム10を接続する。個人情報管理システム10は、登録者毎に、個人情報の閲覧権限を定めた鍵情報を発行する。ある登録者Aが他の登録者Bの個人情報を閲覧したい場合は、その登録者Bに自分の鍵情報を渡して登録者Bからその者の鍵情報を受け取る。個人情報管理システム10は、受け取った鍵情報のレベルに応じて登録者Aによる登録者Bの個人情報の閲覧を許容する。



## 【特許請求の範囲】

【請求項 1】 不特定者がアクセス可能なシステムに於いて実行される方法であって、  
前記不特定者からの個人情報の登録を受け付ける過程と、

個人情報を登録した登録者毎に定めた領域に、その者の個人情報の閲覧を許容する相手を識別するための所定の識別情報を記録する過程と、

前記相手から前記識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする過程とを含み、

前記識別情報の記録を個々の登録者の行為に起因して行うことを特徴とする、個人情報管理方法。

【請求項 2】 閲覧を許容し得る個人情報の範囲を複数範囲設定しておき、前記閲覧要求があった場合に、前記識別情報によって定めたいずれかの範囲の個人情報の閲覧を可能にすることを特徴とする、

請求項 1 記載の個人情報管理方法。

【請求項 3】 前記複数の範囲の各々にそれぞれ異なる鍵情報に対応づけるとともに前記識別情報にいずれかの鍵情報を含ませておき、前記閲覧要求があった場合に、前記識別情報に含まれる鍵情報によって特定される範囲の個人情報の閲覧を可能にすることを特徴とする、

請求項 2 記載の個人情報管理方法。

【請求項 4】 閲覧を許容し得る個人情報の範囲を階層的に選択できるようにしておき、前記閲覧要求があった場合に、選択された層の個人情報の閲覧を可能にすることを特徴とする、

請求項 1 記載の個人情報管理方法。

【請求項 5】 各々の登録者に自己の前記領域の参照を許容するとともに、前記識別情報の記録に代えて、あるいは該識別情報と共に、当該識別情報に対応する所定のアイコンを記録して、当該領域の記録情報を視認可能にすることを特徴とする、

請求項 1 記載の個人情報管理方法。

【請求項 6】 それぞれ同一の者の識別情報が記録されている複数の前記領域を相互に関連付けておき、これらの領域から特定される個々の登録者の接続情報の一部又は全部を当該領域によって関連付けられた登録者間で共有することを特徴とする、

請求項 1 ないし 5 のいずれかの項記載の個人情報管理方法。

【請求項 7】 不特定の者がアクセス可能なネットワーク上に、所定の識別情報によって閲覧可能な範囲が定まる登録者の個人情報を登録する過程と、

前記登録者が前記識別情報を自分の個人情報を閲覧させたい相手に渡した時点で最低限の範囲の個人情報を閲覧可能な状態にするとともに前記ネットワークを通じて前記相手から前記識別情報を伴う個人情報の閲覧要求があった場合に前記閲覧可能な状態にある個人情報の範囲を

拡大させる過程とを含む、  
個人情報管理方法。

【請求項 8】 不特定者がアクセス可能なネットワークに接続されるシステムであって、

前記ネットワークを通じて不特定者から受け付けた個人情報を登録するとともに、この個人情報を登録した登録者毎に、自分の個人情報を閲覧させたい相手を識別するための所定の識別情報が記録される領域を用意する登録管理手段と、

10 前記ネットワークを通じて前記相手から前記識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする閲覧管理手段とを備えることを特徴とする、

個人情報管理システム。

【請求項 9】 いずれかの登録者からの個人情報が修正された場合に当該登録者の個人情報が関わるシステム内のすべての記録情報を前記個人情報の修正内容に応じて修正する手段と、

前記修正後の個人情報にアクセス可能なすべての登録者宛に当該個人情報が修正された旨を電子的に通知する手段とをさらに備える、

請求項 8 記載の個人情報管理システム。

【請求項 10】 不特定者がアクセス可能なネットワークに接続されるシステムであって、

前記ネットワークを通じて不特定者から受け付けた個人情報を登録するとともに、この個人情報を登録した登録者毎に用意した接続リストへの情報記録を行う登録管理手段と、

30 前記ネットワークを通じて一の登録者の個人情報に対する閲覧要求を受け付けたときに閲覧要求に応答するかどうかを決定する閲覧管理手段とを備え、

登録者毎の接続リストは、それぞれ自己の個人情報を閲覧させたい相手を識別するための識別情報が当該登録者の行為に起因して記録されるものであり、前記識別情報は閲覧を許容する個人情報の範囲を定める鍵情報を含むものであり、

前記閲覧管理手段は、前記識別情報を伴う一の登録者の個人情報に対する閲覧要求があった場合に当該一の登録者用の接続リストに前記識別情報が記録されていることを条件として当該一の登録者の個人情報の閲覧を前記鍵情報で特定される範囲で可能にすることを特徴とする、

個人情報管理システム。

【請求項 11】 携帯電話、携帯性情報処理端末等の携帯性操作端末との間で通信を行う手段を備え、前記閲覧要求を前記携帯性操作端末から受け付けるように構成されていることを特徴とする、

請求項 8 又は 10 記載の個人情報管理システム。

50 【請求項 12】 不特定者がアクセス可能なネットワークに接続されるコンピュータに、下記の処理を実行させ

## 3

るためのプログラムコードが記録された、コンピュータ読み取り可能な記録媒体。

(1) 前記ネットワークを通じて不特定者から受け付けた個人情報を登録するとともに、この個人情報を登録した登録者毎に、自分の個人情報を閲覧させたい相手を識別するための所定の識別情報が記録される領域を用意する処理、(2) 前記ネットワークを通じて前記相手から前記識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする処理。

【請求項 13】 前記プログラムコードが、さらに下記の処理を実行させるものである、請求項 12 記載の記録媒体。(3) いずれかの登録者の個人情報が修正された場合に当該登録者の個人情報が関わるシステム内のすべての記録情報を前記個人情報の修正内容に応じて修正する処理、(4) 前記修正後の個人情報にアクセス可能なすべての登録者宛に当該個人情報が修正された旨を電子的に通知する処理。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば住所録や名刺等に記載されているような、個人の名前、所属、役職、連絡先その他の個人情報をネットワーク上で効率的に管理するための個人情報管理技術に関する。

【0002】

【発明の背景】自分の個人情報を他人に伝えるアイテムとして、名刺が一般的に使用されている。この名刺の管理は、従来、紙ベースあるいはコンピュータベースのいずれかにより行われている。紙ベースによる管理は、通常は、名刺に記載された情報を住所録に転記することにより行われる。

【0003】紙ベースでの管理は最も簡便な形態である。しかし、名刺数が多くなると、事後的に必要な名刺を探し出したり、住所録から該当情報を特定するのが困難になる。また、名刺は、通常は、初対面の相手に 1 回渡すだけなので、その後の個人情報の変化はわからない。そのため、時間の経過に伴って連絡が途切れてしまい、個人情報の活用が図れない場合が多い。さらに、紙ベースでの管理では、住所録に転記した者が他の者とのようなつながりをもっているかは、把握することができない。

【0004】このような問題を解決する上でコンピュータベースでの管理形態は便利である。コンピュータを用いたこの種の情報の管理手段として、特開平 11-66082 号公報に記載された名刺情報検索装置がある。この名刺情報検索装置では、いずれかのユーザから入力された名刺及びその更新情報をすべてのユーザ間で共有できるようにしておき、また、誰が誰から名刺をもらったかという情報を併せて登録しておくことにより、第三者が他人の人脈情報を得ることができるようになる。名刺

## 4

情報の一部については、第三者に秘匿できるようにすることで、情報のセキュリティ性を確保している。

【0005】しかしながら、上記の名刺情報検索装置は、基本的には個々のユーザの名刺情報の殆どを複数のユーザで共有して公開しあうことである。ユーザによっては、特定の者には情報を公開したいが、他の者についてはその殆どを秘匿したいと願う者もいるだろうし、相手側から情報が得られた場合にその相手を信頼して自分の情報を知らせたいという場面も考えられる。つまり、公開可能な個人情報の範囲を当事者間の信頼関係によって各当事者が自由に決めるようにできれば、より現実的な個人情報の利用形態が実現される知見がある。上記の名刺情報検索装置は、この点を解決することができない。さらに、上記の名刺情報検索装置は、個人情報の受け渡しはコンピュータによって行われることを前提としており、オフライン（名刺のような紙ベースでの情報交換）との連携が考慮されていない。

【0006】最近では、インターネットのような広域ネットワークを媒介として人と人とが知り合う機会も多くなっている。このような状況下では、名刺に代わる個人情報の伝達形態や従来にない個人情報の効率的な管理形態の実現が望まれる。

【0007】本発明は、人と人とが知り合うたびに発生する個人情報の公開範囲を自分の意思でコントロールできるようにする新規な個人情報管理方法を提供することを、主たる課題とする。本発明の他の課題は、自分の個人情報を他人に安全且つ効率的に伝達することができ、他人の個人情報もその他人の了解のもとで確実に知得ることができる、個人情報管理システムを提供することにある。本発明の他の課題は、効率的な個人情報の管理をコンピュータ上で実現するうえで好適となる記録媒体を提供することにある。

【0008】

【課題を解決するための手段】本発明は、不特定者がアクセス可能なシステムに於いて、不特定者からの個人情報の登録を受け付ける過程と、個人情報を登録した登録者毎に定めた領域に、その者の個人情報の閲覧を許容する相手を識別するための所定の識別情報を記録する過程と、前記相手から識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする過程とを少なくとも実行し、前記識別情報の記録を個々の登録者の行為に起因して行う、個人情報管理方法を提供する。上記の過程を経ることにより、登録者は、自分の個人情報を閲覧することができる者を自分の行為に起因して自由に決めることができるようになる。

【0009】閲覧を許容し得る個人情報の範囲を複数範囲設定し、閲覧要求があった場合に、識別情報によって定めたいずれかの範囲の個人情報の閲覧を可能にすることができる。具体的には、複数の個人情報の範囲の各々にそれぞれ異なる鍵情報を対応づけるとともに相手に渡

す識別情報にいずれかの鍵情報を含ませておき、相手からの閲覧要求があった場合に、識別情報に含まれる鍵情報によって特定される範囲の個人情報の閲覧を可能にする。これにより、閲覧させても良い個人情報の範囲を自分の意思で自由にコントロールできるようになる。

【0010】閲覧を許容し得る個人情報の範囲を階層的に選択できるようにしておき、閲覧要求があった場合に、選択された層の個人情報の閲覧を可能にしても良い。このようにすれば、携帯電話や携帯性情報処理端末のように表示スペースが小さい場合であっても、必要な情報を効率的に閲覧させることができる。各々の登録者に自己の前記領域の参照を許容するとともに、識別情報の記録に代えて、あるいは識別情報と共に、当該識別情報に対応する所定のアイコンを記録して、当該領域の記録情報を視認可能にしても良い。この場合は、識別情報の受け渡し状況を各登録者が容易に把握できるようになる。

【0011】それぞれ同一の者の識別情報が記録されている複数の前記領域を相互に関連付けておき、これらの領域から特定される個々の登録者のコネクション情報の一部又は全部を当該領域によって関連付けられた登録者間で共有するようにしても良い。このようにすれば、他人のコネクション情報を用いて登録者同士のつながり

(人脈)を拓けることができる。この場合、自分のコネクション情報が他の登録者によって利用されることについての権限を定めるようにする。

【0012】本発明は、また、不特定の者がアクセス可能なネットワーク上に、識別情報によって閲覧可能な範囲が定まる登録者の個人情報を登録する過程と、登録者が識別情報を自分の個人情報を閲覧させたい相手に渡した時点で最低限の範囲の個人情報を閲覧可能な状態になるとともにネットワークを通じて相手から識別情報を伴う個人情報の閲覧要求があった場合に、閲覧可能な状態にある個人情報の範囲を拡大させる過程とを含む、個人情報管理方法を提供する。この方法では、相手から識別情報を受け取る前でも最低限の個人情報をその相手用に公開するので、相手の便宜が図られる。

【0013】上記の他の課題を解決する本発明の個人情報管理システムは、不特定の者がアクセス可能なネットワークに接続されるシステムであって、ネットワークを通じて不特定者から受け付けた個人情報を登録するとともに、この個人情報を登録した登録者毎に、自分の個人情報を閲覧させたい相手を識別するための所定の識別情報が記録される領域を用意する登録管理手段と、ネットワークを通じて相手から識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする閲覧管理手段とを備えるものである。好ましくは、いずれかの登録者からの個人情報が修正された場合に当該登録者の個人情報が関わるシステム内のすべての記録情報を前記個人情報の修正内容に応じて修正す

る手段と、前記修正後の個人情報にアクセス可能なすべての登録者宛に当該個人情報が修正された旨を電子的に通知する手段とをさらに備えて個人情報管理システムを構成する。これにより、常に最新の個人情報を閲覧可能になる。個人情報を最新のものに修正する責任は、登録者自身が負う。

【0014】本発明は、また、不特定者がアクセス可能なネットワークに接続されるシステムであって、ネットワークを通じて不特定者から受け付けた個人情報を登録するとともに、この個人情報を登録した登録者毎に用意したコネクションリストへの情報記録を行う登録管理手段と、ネットワークを通じて一の登録者の個人情報に対する閲覧要求を受け付けたときに閲覧要求に応答するかどうかを決定する閲覧管理手段とを備える個人情報管理システムを提供する。登録者毎のコネクションリストは、それぞれ自己の個人情報を閲覧させたい相手を識別するための識別情報が当該登録者の行為に起因して記録されるものであり、識別情報は閲覧を許容する個人情報の範囲を定める鍵情報を含むものである。閲覧管理手段は、識別情報を伴う一の登録者の個人情報に対する閲覧要求があった場合に当該一の登録者用のコネクションリストに識別情報が記録されていることを条件として当該一の登録者の個人情報の閲覧を鍵情報で特定される範囲で可能にする。

【0015】本発明は、また、不特定の者がアクセス可能なネットワークに接続されるコンピュータに、下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読み取り可能な記録媒体を提供する。

(1) ネットワークを通じて不特定者から受け付けた個人情報登録するとともに、この個人情報を登録した登録者毎に、自分の個人情報を閲覧させたい相手を識別するための所定の識別情報が記録される領域を用意する処理、(2) ネットワークを通じて相手から識別情報を伴う個人情報の閲覧要求があった場合に、当該相手による当該個人情報の閲覧を可能にする処理。好ましくは、前記プログラムコードが、さらに下記の処理を実行させるものとする。(3) いずれかの登録者の個人情報が修正された場合に当該登録者の個人情報が関わるシステム内のすべての記録情報を個人情報の修正内容に応じて修正する処理、(4) 修正後の個人情報にアクセス可能なすべての登録者宛に当該個人情報が修正された旨を電子的に通知する処理。

【0016】

【発明の実施の形態】以下、本発明を適用した電子住所録管理システムの実施形態を説明する。図1は、この電子住所録管理システムの全体構成図である。電子住所録管理システム1は、ネットワークの一例となるインターネットに、個人情報管理システム10と、不特定者が操作して個人情報管理システム10にアクセスする各種操作端末とを接続して構成される。

【0017】操作端末は、ここでは、データ処理手段付の携帯電話20k、携帯型情報処理端末の一例となる携帯型パソコン20m、スタンドアロン型パソコン20sとする。以下、これらを区別する必要がある場合を除き、この実施形態では、操作端末20と総称する。操作端末20は、それぞれ、HTML言語で書かれたファイルを読み取ることができるブラウザを表示するための表示部を備えるものである。ブラウザとしては、各種パソコン20m、20cの場合には、良く知られているInternetExplore、NetscapeNavigator等を使用することができる。携帯電話20kの場合には、閲覧用ページ画面を携帯電話用のサイズに縮小するとともに画面内容を編集する機能を、後述するサーバ処理部11に設ける。

【0018】個人情報管理システム10は、Webサーバとしての役割を果たすことができるコンピュータによって実現されるもので、このコンピュータが搭載している基本制御プログラム(OS(オペレーティングシステム)やBIOS(基本入出力制御システム)と本発明の記録媒体に記録された各種プログラムコードとの協働によって、図2に示されるような機能ブロック、すなわち、サーバ処理部11、表示制御部12、要求受付部13、登録処理部14、データベース管理システム(DBMS)15を具備するものである。本実施形態で用いるプログラムコードは、「Servlet」という、Java言語でコーディングされた公知のプログラムコードを含む。記録媒体は、CD-ROM、DVD-ROM、半導体メモリのような可搬性記録媒体であっても良いが、運用時に、上記コンピュータが読みとり可能なハードディスク等の固定型記録媒体にOS等と共に記録されるようにしておくことが好ましい。

【0019】サーバ処理部11は、操作端末20との間の通信を制御するものであり、Webサーバソフトウェア又は同等機能ソフトウェア(プログラムコード等)によって実現される。電子メールの発信及び仲介を行うこともできる。操作端末20からのアクセスは、所定の専用フォームのページ画面(HTML文で表現されたもの)をその端末の表示部に表示させ、そのページ画面の該当領域へのデータ入力を受け付けることによって行うことができる。ページ画面は、複数のものが階層的に用意されており、操作端末20からの操作内容に応じてあるいは予め定めた所定の順序で上位階層から下位階層の順にその表示部に表示させる。操作端末20が携帯電話20kの場合には、図9に示されるように、ページ画面のレイアウトを携帯電話20kの表示部に合わせて編集したものを送出する。

【0020】表示制御部12は、サーバ処理部11を通じて操作端末20の表示部に所要のページ画面が正常に表示されるように制御する。そのために、表示制御部12は、操作端末20の種別毎のパラメータを保持している。要求受付部13は、サーバ処理部11(ページ画

面)を通じて入力された操作端末20からの各種要求を受け付ける。要求には、個人情報の登録の要求、項目や登録事項の削除を含む修正の要求、閲覧の要求がある。登録要求の場合には、登録すべき個人情報の入力を促すためのページ画面が操作端末20の表示部に表示されるようにする。修正の要求、閲覧の要求についても同様である。サーバ処理部11～要求受付部13までは、「Servlet」という、Java言語でコーディングされた公知のプログラムを読み込み、操作端末20の操作

者からの要求内容を判断して、その結果を返信する処理を実行することで、実現が可能である。登録処理部14は、認証処理を含む、個人情報の登録に関する処理を行う。これについては、後述する。

【0021】DBMS15は、データベース(DB)152とその入出力制御部151とから成る。DB152には、ユーザから個人情報の登録を受け付けるたびに更新される登録者テーブルT1と、登録者毎に生成される、基本情報テーブルT2、会社情報テーブルT3、学校情報テーブルT4、プライベート情報テーブルT5、及びコネクションリストCNLが格納される。各テーブルT1～T5は相互にリンクしており、いずれかのテーブルの記録情報をもとに他のテーブルの記録情報を読み出せるようになっている。

【0022】登録者テーブルT1には、システムがすべての登録者を管理できるようにするための管理情報が記録される。具体的には、登録受付時に登録者毎に付与される固有ID、登録者が定めたパスワード、登録者の名前、ふりがな、登録者のメールアドレス等が一覧形式で記録される。基本情報テーブルT2は、登録者の基本情報が記録される。具体的には、登録者の名前又はハンドル名、生年月日、性別、職業、出身地、住所、携帯電話番号、自宅電話番号、自宅FAX番号、メールアドレス等が記録される。会社情報テーブルT3には、登録者の会社に関する情報が記録される。具体的には、登録者の名前、ふりがな、会社名、部署、役職、会社住所、会社電話番号、会社FAX番号、会社メールアドレス、会社ホームページ、勤務時間帯、コメント等が記録される。学校情報テーブルT4には、登録者の出身校や専門分野に関する情報が記録される。具体的には、学校名、学部名、専攻、学年、クラス、部活、サークル、ゼミ、研究室、入学年度、卒業年度、学校メールアドレス、学校ホームページ、コメント等が記録される。プライベート情報テーブルT5には、登録者のプライベートな情報が記録される。具体的には、登録者の顔写真、個人のホームページ、本人の特徴、遊びに行く場所、良く聴く音楽、好きな食べ物、好きなスポーツ、その他のフリー情報等が記録される。

【0023】コネクションリストCNLは登録者個人の住所録として利用されるもので、自分とつながりをもつ他の登録者の固有IDその他の情報が記録される。シス

テム的には、自己の個人情報を閲覧させたい相手（他の登録者）が誰で、どの範囲の情報を閲覧させるかを識別するための識別情報を記録するための、登録者毎に用意された領域として利用される。コネクションリストCNLへの識別情報の記録は、登録者が自分の個人情報を閲覧させたい相手に識別情報を配った事実を自ら入力した場合、システムが他の登録者からその登録者（コネクションリストが対応する登録者）への情報の送出手続きが行われる。他の登録者からの情報の送出手続きが可能になるのは、自分がインターネットLを通じて、あるいはオフラインによって識別情報を他の登録者に渡したことに因る。つまり、コネクションリストCNLへの識別情報の記録は、すべて当該登録者の行為に起因することになる。

【0024】電子住所録システム1では、登録者が自分の個人情報の閲覧を許容する範囲を用途に応じて複数範囲設定しておく。そして、閲覧させたい相手からの閲覧要求があったときに、要求範囲の個人情報を、その相手が操作する操作端末20の画面上に表示させる。「用途に応じて」とは、大枠ではビジネス用途かプライベート用途かを意味する。より詳細な用途を決めることができることは勿論である。用途の切り分けは、基本的には、登録者が、自分の意思によって、自分のコネクションリストCNLに、用途を識別するためのデータを記録しておけば良い。より簡便には、閲覧を許容し得るレベルを定めた鍵情報を定め、それを固有IDと共に識別情報の一例として発行する。鍵情報と閲覧を許容する範囲の設定の仕方は、様々の態様が考えられる。レベルを定めて、各レベルで対象となる情報毎に絞っても良いし、テーブル毎に定めても良い。

【0025】前者の場合（情報毎に絞る場合）は、テーブルの種類に関わらず、例えば3段階のレベルを設定し、レベル1では、名前、性別、職業、出身地、住んでいる都道府県、会社情報テーブルT3に記録された情報のすべてを閲覧許容範囲とし、レベル2では、レベル1の情報に加えて、個人のメールアドレス、携帯電話の番号、生年月日、学校情報テーブルT4に記録された情報のすべてを閲覧許容範囲とする。レベル3は、登録されている個人情報のすべてを閲覧許容範囲とする。デフォルトで、これらの3つのレベルによる個人情報の絞り込みの範囲を上記のように定めておき、これを事後的に変更できるようにしても良い。何を各レベルの個人情報とするかは、登録時に登録者が任意に定める。

【0026】後者の場合（テーブル毎に定める場合）は、例えば基本情報テーブルT2～プライベート情報テーブルT5の各々に、異なるレベルの閲覧権限を表す鍵情報を割り当てる。または、テーブル内の情報項目毎に、その内容を公開するかしないかを設定する。これらも、登録者が任意に定める。「公開しない」を設定する場合は、固有IDの他に相手の鍵情報を受け取らない限

り、その相手に同種の内容を公開しないようにする。つまり、「公開する」者同士は、どちらかが鍵情報を渡せば両者共に情報を閲覧できるが、「公開しない」者に鍵情報を渡した場合は、相手から鍵情報が渡されない限り、相手の情報を閲覧できない。

【0027】後者の場合の鍵情報の割り当ての例を示したのが図3である。基本情報テーブルT2内の情報は、より多くの登録者が本システムを利用できるようにするため、最低限のレベルの鍵情報とする。次の権限レベルの鍵情報では、会社情報テーブルT3までを閲覧することができる。さらに次の権限レベルの鍵情報では、会社情報テーブルT3のほか、学校情報テーブルT4の内容をも閲覧することができる。但し、学校情報テーブルT4については「公開しない」が設定されているので、相手から同レベルの鍵情報を受け取らない限り、実質的に相手は閲覧することができない。それ以上の権限レベルの鍵情報では、プライベート情報テーブルT5の内容をも閲覧することができる。どの部分がどの権限レベルとするかは、親交の度合いによって決める。

【0028】図4(a)、(b)は、識別情報を固有IDと鍵情報とした場合の、ある登録者（登録者Aとする）用のコネクションリストCNLの具体的な内容例を示す図である。コネクションリストCNLの項目としては、自分とつながりをもつ他の登録者の名前Q1、メールアドレスQ2、電話番号Q3、固有IDQ4、最新更新日Q5、渡した鍵情報の種類Q6、受領した鍵情報の種類Q7である。図4(a)は、登録者Aのある時点における鍵情報の受け渡し状況、同(b)は、その後鍵情報の受け渡しがあった場合の状況を、それぞれ示している。「鍵情報を渡した」、「鍵情報を受領した」とは、それぞれ相手の固有IDを追加登録したことを意味する。

【0029】他の登録者の情報を追加すると、フィールドが一つ増え、ID欄に相手の固有IDが記録される。鍵情報を渡した場合は、「渡した鍵情報」の欄に、鍵情報のレベルを表すアイコンが表示されるようにする。

「受領鍵情報」の欄は、その相手から鍵情報を受領するまでは、空欄となる。鍵情報を受領した場合は、そのフィールドの「名前」に相手の名前や「メール」の欄にメールアドレスが加わり、「受領鍵情報」の欄に受け取った鍵情報のアイコンが加わる。なお、図4(b)の最下段のフィールドは、相手からの鍵情報の受領が先行した場合である。相手から鍵情報の受領があった場合は、自動的にフィールドが作成され、鍵情報と相手の情報が記録される。最終的に受け渡しが成立した場合は、両方の鍵情報の欄にアイコンが記録される。これにより、各登録者は、コネクションリストCNLを参照することにより、現在の鍵情報の受け渡し状況を把握し、閲覧可能な者と閲覧可能な個人情報の範囲を確認することができる。

【0030】<運用形態>次に、電子住所録管理システム1の運用形態の一例を説明する。電子住所録管理システム1では、個人情報管理システム10を個人情報の登録、修正（個人情報の内容変更のほか、ID追加登録、鍵情報登録、脱会を含む）、閲覧の窓口としておき、新規登録を行う者、既に登録した者、脱会しようとする者からの各種要求を受け付ける。これらの要求は、通常はインターネットLを通じて行うが、個人情報管理システム10の前で直接それを行う場合もある。個人情報管理システム10の管理者による代理受付も可能である。以下、インターネットLを通じて不特定者からアクセスが行われることを前提として、個人情報管理システム10における登録、閲覧、修正の処理手順を説明する。

#### 【0031】（1）情報登録

新規に自分の個人情報を登録しようとする者は、操作端末20を操作して個人情報管理システム10に登録要求を行う。図5は、個人情報管理システム10における新規登録時の処理手順図である。図5において、個人情報管理システム10は、登録要求を受けて登録用フォームを生成し、これを操作端末20のブラウザ画面上に提示する（R101：Yes、R102）。登録用フォームには、次回以降のアクセスの認証を受けるためのパスワードのほか、必要最低限の個人情報の記入フィールドが形成される。必要最低限の個人情報は、閲覧権限を要しない情報、例えば名前、ふりがな、メールアドレスである。登録フォームの記入フィールドにデータが入力された場合は、これを受け付け（R103）、固有IDを発行する（R104）。受け付けた個人情報は、固有IDと対応付けてDBMS15に登録しておく（R105）。

【0032】登録者が、詳細な個人情報の登録をも行う場合は、詳細情報登録用フォームを生成し、これをブラウザ画面上に提示する（R106：Yes、R107）。上記と同様に、詳細情報が入力されたときは、その登録を受け付ける（R108）。詳細情報は、図3に示したように、会社情報、学校情報、プライベート情報に分けられている。この運用形態では、テーブルT2～T5の種類に関わらず、情報の範囲毎に、それぞれ、異なるレベルの鍵情報を割り当てる（R109）。前述のように、デフォルトで、レベル1～レベル3のいずれかを表す鍵情報を割り当て、詳細は事後的に変更するにしても良い。情報を公開する／しないも、ここで設定する。なお、相手に鍵情報を渡し、鍵情報を渡される前に、デフォルトで、情報の公開をする、という設定もできる。

【0033】鍵情報を相手に渡した場合は、鍵情報のレベルと、渡した相手の固有IDとをDBMSにまとめて登録しておく（R110）。鍵情報を渡した者には、その旨がシステムから通知される。Web上に公開される場合もある。他の詳細情報がある場合は、R107以降

の処理を繰り返し（R111：Yes）、登録処理を終えた後は、トップページ画面をブラウザ画面に表示させる。

【0034】DB152内には、図4に示したようなコネクションリストCNLが、その登録者用に自動生成される。このコネクションリストCNLは、随時、登録者が参照できるようになっている。

#### 【0035】（2）情報検索（閲覧）

図6は、閲覧時の処理手順図である。閲覧要求を受けた場合、個人情報管理システム10は、登録処理部14で登録者認証を行う。登録者認証は、アクセスしてきた者の固有IDとパスワードがそれぞれ予め登録されているものと一致するかどうかにより行う。認証がOKの場合は、閲覧要求を行った登録者用のコネクションリストCNL内のすべての手持ちID（他の者の固有ID）を探索し（S101：Yes、S102）、各手持ちIDに対応する個人情報を特定する（S103）。

【0036】特定した個人情報のうち検査項目にヒットする情報を見つけた場合、例えば該当する名前を見つけた場合は（S104：Yes）、それが検索の初回処理であればHTMLヘッダを作成した後、HTML文を追加作成する（ステップS105：Yes、S106、S107）。初回処理でない場合はHTMLヘッダの作成をパスしてHTML文を追加作成する（ステップS105：No、S107）。名前等のリンクは、HTML文の<A>タグ（登録者Aの場合）内に随時追加する。他の検索項目がある場合はステップS104以降の処理を繰り返す（ステップS108：Yes）。検索項目がなくなった場合は、HTMLフッタを作成して検索処理を終える（S108：No、S109）。検索結果は、随時、ブラウザ画面に表示させる。これにより、閲覧要求を行った者が検索結果を閲覧できるようになる。

【0037】他人から固有IDや鍵情報を受け取った場合のように、閲覧したい個人情報が予め決まっている場合は、操作端末20から個人情報管理システム10に、その情報にアクセスするためのブラウザ画面の表示要求を行う。このとき、相手の固有IDや鍵情報を添付する。ブラウザ画面には、その相手のどの情報を得たいのかを選択するための専用フォームが形成されている。個人情報管理システム10は、DB152内の該当者のテーブルT2～T5にアクセスし、個人情報を引き出して良いかどうかという項目のチェックを行う。チェックは、例えば上述の「Servlet」を起動することにより行う。チェックがOKであれば、その相手の個人情報を引き出し、要求した登録者のブラウザ画面に表示させる。

#### 【0038】（3）情報修正

既に登録してある個人情報は、随時修正することができる。例えば登録者の名前、住所、会社等が替わった場合、登録者が特定者への情報の公開を中止したい場合、

脱会したい場合は、登録者が自分の固有IDを添えて個人情報管理システム10に修正要求を行う。図7は、個人情報管理システム10における個人情報修正時の処理手順図であり、個人情報の部分修正の場合の例を示している。

【0039】修正要求を受けた場合は、個人情報管理システム10は、閲覧要求時と同様の登録者認証を行い、OKであれば、DBMS15からその登録者の個人情報を引き出してブラウザ画面に提示する(K101: Yes, K102)。そのブラウザ画面を通じて修正内容が入力された場合は、それを受け付け(K103)、その登録者の個人情報を更新する(K104)。その後、修正要求を行った登録者の個人情報を登録(使用)している他の登録者がいるかどうかを調べる(K105)。他の登録者がいる場合は、その登録者の固有IDを特定し(K105: Yes, K106)、特定したすべての登録者に情報更新通知を行う(K107)。すべての登録者が見る掲示板やページ画面に、一括通知するような形態も可能である。その後、修正要求を行った登録者に更新完了通知を行って修正処理を終える(K108)。

【0040】脱会の場合には、上記の各通知の後、脱会した登録者に関するすべてのテーブル、リストを削除する。また、脱会した登録者が渡したすべての鍵情報を削除し、一連の処理が完了した場合は、その旨を脱会要求者に伝える。

【0041】個人情報管理システム10では、すべての登録者の個人情報を集中的に記録しているため、上記のような内容変更があった場合は、その個人情報に関わるシステム内のすべての記録情報を修正する。この場合は、他の登録者にとっては、自分の意思によらない変更が生じたことになるので、それらの者に変更があった旨をトップページ画面等を通じて電子的に通知する。

【0042】このように、個人情報管理システム10では、一の登録者が他の登録者に識別情報を渡したときに当該他の登録者用のコネクションリストCNLに一の登録者の固有IDと当該鍵情報とを記録しておき、いずれかの登録者からの閲覧要求に対して、当該登録者用のコネクションリストCNLに記録されている情報に基づく閲覧を許可する処理を行うようにしたので、不特定者がアクセスし得る環境下に自分の個人情報をおいた場合であっても、セキュリティ性を維持することができる。

【0043】また、このような環境下に自分の個人情報をおくことで、インターネットを通じて自己紹介したり、相手の個人情報を知ることがきわめて容易になり、コミュニティの場を拡げることができるようになる。各登録者のコネクションリストCNLの内容に変更があった場合は、随時それが修正され、関係者に通知されるので、個人情報が替わった場合であっても、名刺による個人情報管理のように、連絡が途絶えることがなくなる。

【0044】また、コネクションリストCNLに相手の

固有IDと鍵情報のアイコンを記録してそれぞれの登録者に提示するようにしたので、登録者は、現在の自分の鍵情報の受け渡し状況や相手からの受け取り状況を視覚的に任意の時点で知ることができるようになる。

【0045】さらに、各登録者の個人情報の閲覧可能範囲が複数範囲設定され、閲覧可能範囲毎について異なるレベルの鍵情報が割り当てられるので、相手に伝えたい情報の範囲とある相手には秘密にしたい情報範囲とを自分の意思でコントロールすることができるようになる。

10 【0046】次に、本実施形態の電子住所録管理システム1の使用例を説明する。

<使用例1>まず、図8を参照して、携帯型パソコン20mを用いて登録者Aが登録者Bの個人情報を閲覧する場合の使用例を説明する。前提として、図8最上段に示されるように、登録者A、Bが、それぞれ自分の固有IDをオフライン又はオンラインで交換しあい、相手側の固有IDを知っているものとする。この状況では、登録者A、Bは、それぞれ相手の固有IDを用いて個人情報管理システム10にアクセス(検索要求)することで、  
20 相手の最低限の個人情報を閲覧することができる。

【0047】登録者Aが自分のコネクションリストCNLに登録者Bの固有IDを追加すると、登録者Bに関する情報、例えば登録者Bの名前等が、自分のコネクションリストCNLに自動的に転記される。登録者Aは、登録者Bの個人情報をより詳細に閲覧したい場合は、登録者Bに自分の鍵情報を渡す。鍵情報の受け渡しは、Web又は電子メールにより行うことができる。また、鍵情報を渡した旨を、自分のコネクションリストCNLに追加する。この段階では、登録者Aは、登録者Bの詳細情報を見ることはできない。

30 【0048】登録者BのコネクションリストCNLには、図4(b)の最下段のように、登録者Aから鍵情報が渡されたことを知らせるアイコンが自動的に記録される。登録者Bは、アクセス時に自分のコネクションリストCNLを見て、あるいは電子メールやWebを通じて通知されたことをもって、登録者Aから鍵情報が届いたことを知る。

40 【0049】登録者Bは、登録者Aに自分の詳細情報を閲覧させて良いと判断した場合は、登録者Aに鍵情報を渡す。そして、鍵情報を渡した旨を自分(B)のコネクションリストCNLに記録する。すると、登録者AのコネクションリストCNLのうち、先に追加形成されている登録者Bの「受領欄」に、登録者Bから鍵情報を受領したことを示すアイコンが自動的に記録される。これにより、登録者A、B共に鍵情報で特定される分だけの相手の個人情報を閲覧できるようになる。

50 【0050】なお、上記の使用例では、固有IDと鍵情報とを別々に受け渡すことによって、各々の個人情報を閲覧できるようにしたが、固有IDと鍵情報とを同時に相手側に渡すようにしても良い。すなわち、登録者Aが

AからBの  
鍵情報  
を渡す  
アクセス



自分の個人情報を閲覧させたい登録者Bに、自分の固有IDと鍵情報とを同時に渡す。登録者Bから鍵情報を受け取るまでは、最低限の範囲の個人情報のみの閲覧を許容する。これは、一々鍵情報を受け渡すまでもなく、公開しても良いと判断した項目については、公開しておいた方が相手の便宜にもなるし、以後の処理も軽減されることによる。

【0051】<使用例2>次に、登録者Aが、登録者Cの個人情報を携帯電話20kを用いて閲覧する場合の例を説明する。図9は、この場合の携帯電話20kの画面の遷移例を示した図である。登録者Aは、自己の固有IDとパスワードとを個人情報管理システム10に送出し、認証を受けることで、本システムの利用画面を表示させることができる。図9左上の例では、自己が要求し得る内容が階層的に表現され、選択された層の個人情報が画面上に表示されるようになっている。図示の例では、[4]住所録が登録者Aによって選択されている。

「住所録」では、図4に示したコネクションリストCNLの項目(Q1~Q7)と、住所録検索のための項目とが選択できるようになっている。「住所録」の下位の階層の「名前一覧」を選択すると、コネクションリストCNLの「名前」の項目Q1が選択され、特定の名前を選択すると、その名前の登録者の詳細情報の閲覧要求とその表示ができるようになっている。このような画面の表示の仕方を採用することにより、表示部の画面サイズが小さい携帯電話20kであっても、必要な情報を効率的に閲覧できるようになる。

【0052】<他の実施形態>上記の実施形態では、固有ID及び鍵情報を受け渡すことによって、各々の個人情報を閲覧できるようにしたが、セキュリティ性が特に要求されない用途では、鍵情報を用いず、固有IDの受け渡しのみで、個人情報の閲覧を可能にすることも可能である。この場合は、個人情報管理システム10で、一の登録者が他の登録者に自己の固有IDを渡したときに当該他の登録者用のコネクションリストCNLに一の登録者の固有IDを記録する。また、一の登録者が他の登録者から固有IDを受け取ったときに当該一の登録者用のコネクションリストCNLに他の登録者の固有IDを記録する。そして、いずれかの登録者からの閲覧要求に対して、当該登録者用のコネクションリストCNLに記録されている固有IDによって特定される個人情報の閲覧を許容する。このようにすれば、より簡易にコミュニティの場を構築できるようになる。

【0053】<他の実施形態>また、個々の登録者のコネクションリストCNLをより有効に活用して、ネットワークにおけるコミュニティの場を拡大したり、複数の個人情報を統合して、それを戦略面に利用したりする形態も可能である。すなわち、同一の登録者との間で鍵情報の受け渡しを行ったすべての者用のコネクションリストCNLを相互に関連付けておき、ある登録者のコネク

ション情報(人脈の情報)の一部又は全部を他の複数の登録者との間で共有できるようにする。コネクションリストCNLの関連付けは、例えば、同一の固有ID同士をリンクさせることで実現することができる。コネクション情報の共有は、具体的には、リンクがはられたすべての登録者が他の登録者用のコネクションリストCNLの内容を参照できるようにすることを意味する。このようにすれば、例えば100人の登録者が、それぞれ10人の他の登録者とつながりがある場合に、1000人分(100人×10人)の個人情報にアクセスできるようになる。

【0054】このような形態による利点としては、例えば、以下のようなものが挙げられる。登録者Aが現在進めている商談が難航している。しかし、先方の担当者は、同社社員(この者も登録者)である登録者D(登録者AのコネクションリストCNLに記録されている登録者)の学生時代の後輩であることが、その登録者DのコネクションリストCNLと、そのコネクションリストCNLに登録されている担当者の学校情報を参照することによって判明した。そこで、登録者Dを通じて先方の担当者とコネクションをとってもらい、商談を成立させる。

【0055】<他の実施形態>コネクションリストCNLを操作端末20とDBMS15との双方で管理し、いずれかに変更が生じた場合に他方を修正するような形態も可能である。すなわち、通常は、操作端末20側のコネクションリストCNLを住所録として使用し、誰にどの鍵情報を渡したか等は、操作端末20の側で管理し、オンラインで個人情報管理システム10と接続した場合に、両者の一致性をみる。不一致の項目がある場合は、最新の情報をそれ以前の情報に反映させるようにする。電子メールやWeb上に、その旨(不一致の旨)を公開するようにしても良い。

【0056】なお、以上の実施形態は、例示であって、上記の機能ブロック、その実現手段及び処理手順に限定する趣旨ではない。上記の説明では、中心的な処理動作を行うのは一つの個人情報管理システム10であったが、個人情報管理システム10と同等の機能を実現する複数の情報処理システムも本発明の範囲である。

【0057】

【発明の効果】以上の説明から明らかなように、本発明によれば、自分の個人情報が公開される範囲を自分の意思でコントロールするための効率的な管理が可能になるという特有の効果が得られる。また、自分の個人情報を、安全且つ効率的に他人に伝達することができ、他人の個人情報も、その他人の了解のもとで用意に知得することができるという、効果も得られる。

【図面の簡単な説明】

【図1】本発明を適用した電子住所録管理システムの全体構成図。

17

【図 2】本発明の一実施形態による個人情報管理システムの機能ブロック図。

【図 3】個人情報の開示可能範囲と、各範囲毎に定めた鍵情報との関係を示した説明図。

【図 4】コネクションリストの内容例を示した図で、  
(a) はある時点での内容、(b) は、他の登録者との間で鍵情報の受け渡しがあった時点での内容を示している。

【図 5】個人情報管理システムにおける、個人情報の新規登録時の処理手順説明図。

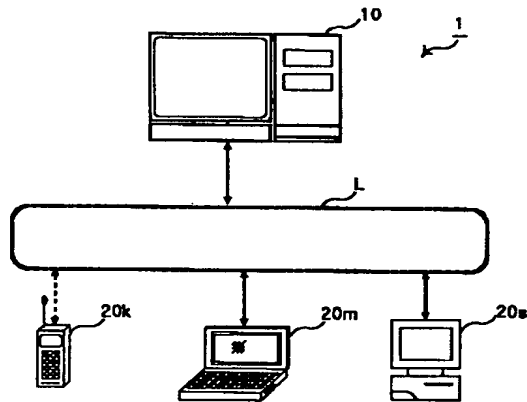
【図 6】個人情報管理システムにおける、個人情報検索時の処理手順説明図。

【図 7】個人情報管理システムにおける、個人情報修正時の処理手順説明図。

【図 8】電子住所録管理システムの使用例を示した説明図。

【図 9】本発明を携帯電話を用いて実施する場合の携帯

【図 1】



18

電話の表示画面の遷移例を示した図。

【符号の説明】

1 電子住所録管理システム

10 個人情報管理システム

11 サーバ処理部

12 表示制御部

13 要求受付部

14 登録処理部

15 DBMS

10 151 入出力制御部

152 DB

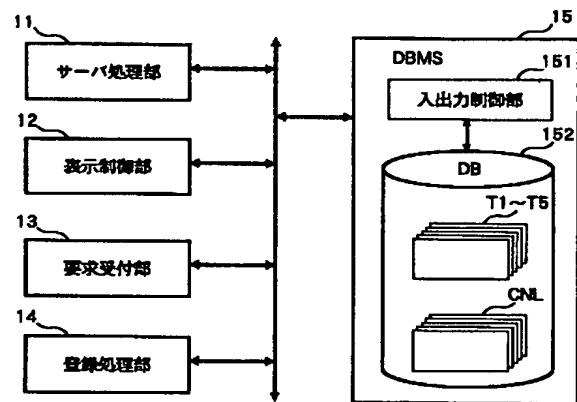
20、20k、20m、20s 操作端末（携帯電話、携帯型パソコン、据え置き型パソコン）

L インターネット

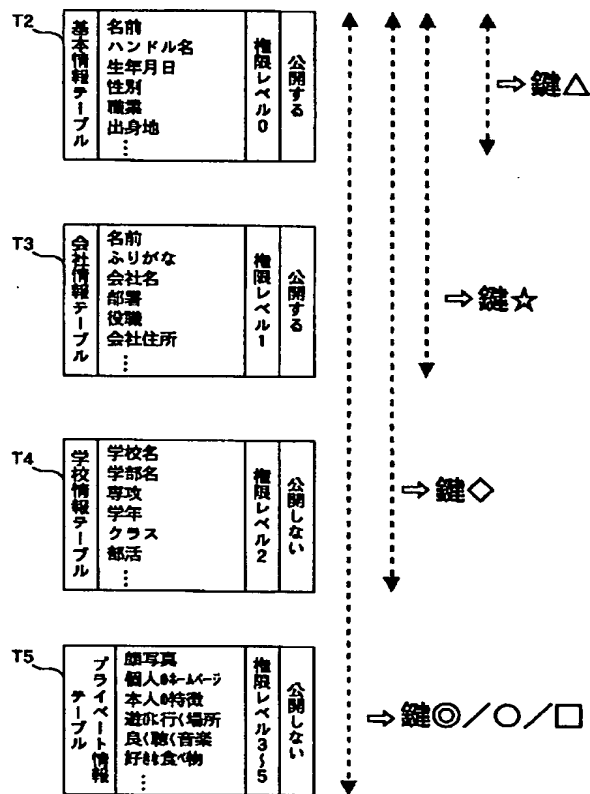
T1、T2～T5 個人情報に関わる情報が記録されたテーブル

CNL コネクションリスト

【図 2】



【図3】



【図4】

(a)

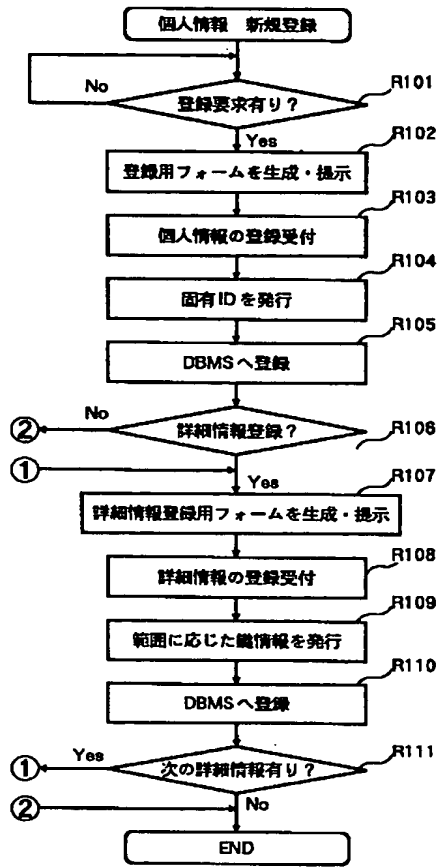
名前	メール	電話番号	ID	更新日	渡した鍵	受信鍵
B	ab@a.org	*****	ae1110	000620	◎	●
C	d@a.com	*****	ae0025	000601	☆	★
D	fg@h.com	*****	ae0022	000618	◎	●
E	ij@k.com	*****	ae1023	000630	○	
F	lm@n.org	*****	ae0020	000610	○	

(b)

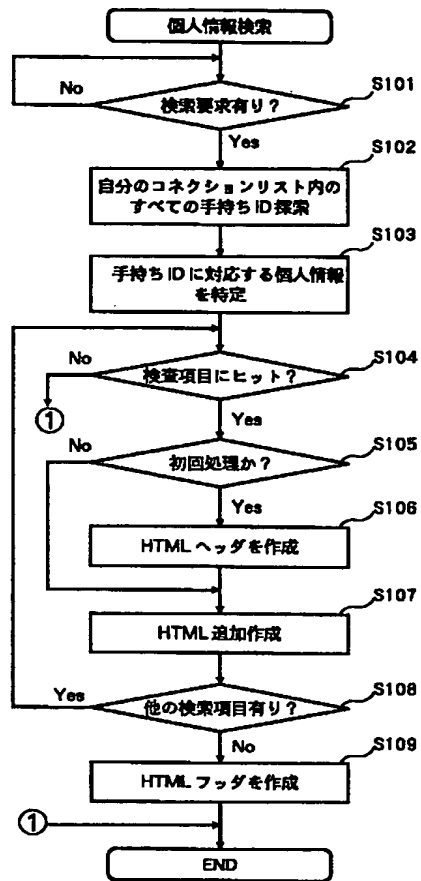
名前	メール	電話番号	ID	更新日	渡した鍵	受信鍵
B	ab@a.org	*****	ae1110	000620	◎	●
C	d@a.com	*****	ae0025	000601	☆	★
D	fg@h.com	*****	ae0022	000618	◎	●
E	ij@k.com	*****	ae1023	000620	○	
F	lm@n.org	*****	ae0020	000610	○	
G	op@q.com	*****	ae1220	000630	◎	
H	rs@t.com	*****	ae1230	000630		●

追加 (Addition) is indicated for rows G and H in table (b).

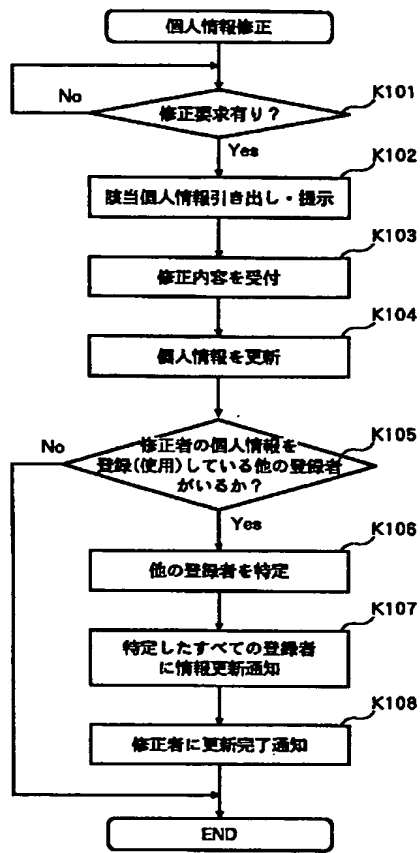
【図 5】



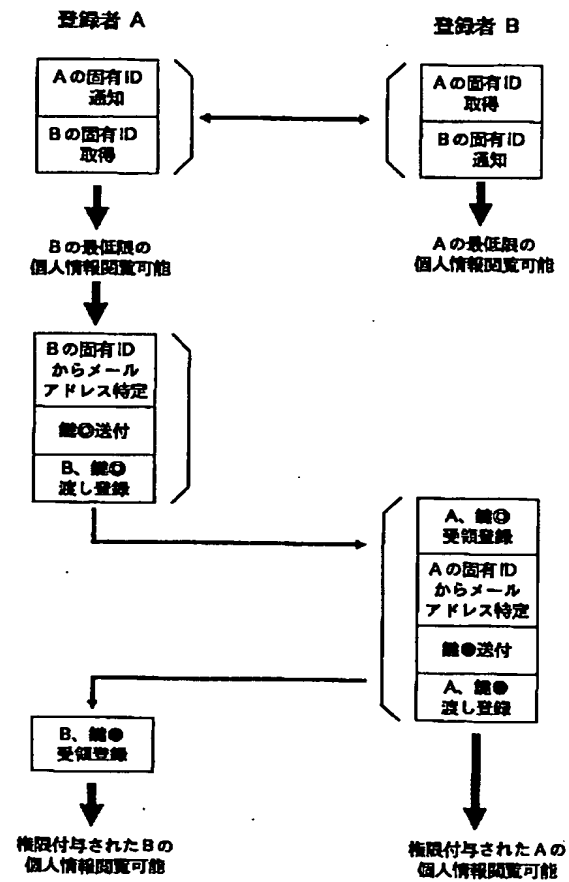
【図 6】



【図 7】



【図 8】



【図9】

